PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 3 : G07F 7/10

A1

(11) International Publication Number: WO 83/ 03018

(43) International Publication Date: 1 September 1983 (01.09.83)

(21) International Application Number: PCT/SE83/00062

(22) International Filing Date: 24 February 1983 (24.02.83)

(31) Priority Application Number: 411/82

(32) Priority Date: 25 February 1982 (25.02.82)

(33) Priority Country: IE

(71) Applicant: TELEFONAKTIEBOLAGET L M ERICSSON [SE/SE]; S-126 25 Stockholm (SE).

(72) Inventors: CREMIN, Patrick, Victor ; 43 Kilgobbin Heights, Stepaside, County Dublin (IE). CARROLL, Patrick, Gerard ; Richardstown House, Kildangin, Monasterevin, Co. Kildare (IE).

(74) Agents: GAMSTORP, Bengt et al.; Telefonaktiebolaget L M Ericsson, S-126 25 Sotckholm (SE).

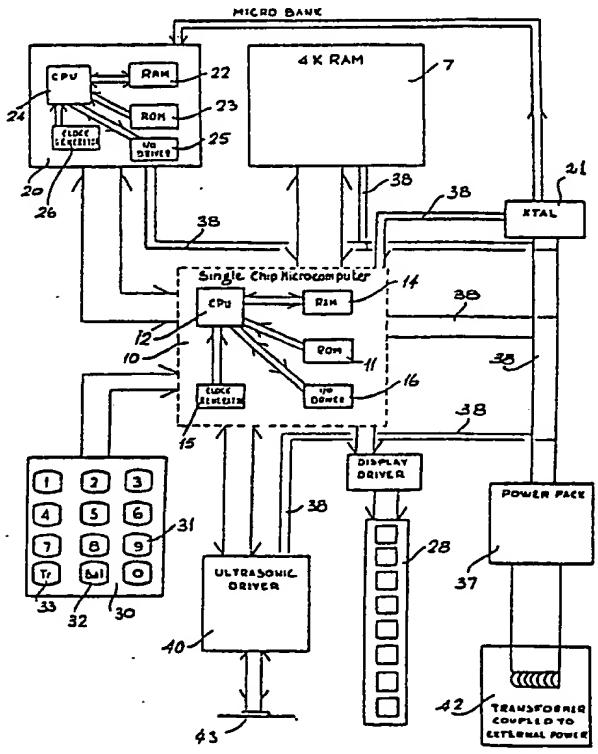
(81) Designated States: AT (European patent), AU, BE (European patent), CH (European patent), DE (European patent), DK, FI, FR (European patent), GB (European patent), JP, LU (European patent), NL (European patent), NO, SE (European patent).

Published
With international search report.

(54) Title: A PORTABLE DEVICE FOR STORING AND TRANSFERRING DATA

(57) Abstract

A portable device for storing and transferring funds for use in a funds transfer system. Each portable device (1) is card-like and comprises a memory means (7) for storing a monetary balance, and a plurality of identifying characteristics of the user. Micro-computer means (10) in the card (1) update the balance after funds transfer, and randomly select some of the identifying characteristics to query the user. The users response is compared with the stored characteristics. Ultra-sonic coupling means (40) in the card permits coupling to another card (1) through a coupling terminal (2). A keyboard (30) and a digital display (28) permit inspection of the balance. The micro-computer (10) date and time stamps each transaction.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria
AU	Australia
BE	Belgium
BR	Brazil
CF	Central African Republic
CG	Congo
CH	Switzerland
CM	Cameroon
DE	Germany, Federal Republic of
DK	Denmark
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
HU	Hungary
JP	Japan
KP	Democratic People's Republic of Korea
LI	Liechtenstein
LK	Sri Lanka
LU	Luxembourg
MC	Monaco
MG	Madagascar
MR	Mauritania
MW	Malawi
NL	Netherlands
NO	Norway
RO	Romania
SE	Sweden
SN	Senegal
SU	Soviet Union
TD	Chad
TG	Togo
US	United States of America

A PORTABLE DEVICE FOR STORING AND TRANSFERRING DATA

The present invention relates to a portable device for storing and transferring data, the device being of the type comprising memory means for storing the data and an identifying characteristic to prevent unauthorised use of the device, coupling means for coupling the device to an external terminal or other device for transferring data, micro-computer means to update the data in the device after data transfer, means to compare an identifying characteristic entered by the user with the identifying characteristic stored in the memory means, and clock means to drive the micro-computer.

Such devices are well known, and generally are in the form of a substantially flat pocket sized card. A monetary balance or any other data may be stored in the device, and transferred to another device. A coupling terminal is normally provided for routing the data being transferred and the two portable devices between which a transaction is to be made are connected into the coupling terminal. U.S. Patent Specifications Nos. 4,211,919, 4,102,493, 4,092,524, 4,007,355, 4,001,550 and 3,971,916 describe such devices and terminals.

Unfortunately, these known devices suffer from various disadvantages, particularly, in the field of security,both of the device and the information stored therein, and during transfer of the data. Furthermore, due to the fact that most devices need to be connected on line or into a computer, they lack versatility.

In particular, where security is concerned, none of the known devices are secure against unauthorised use. Most rely on the use of a personal identification number stored in the memory of the card, and once the correct personal identification number is proveded by the user, the card is enabled to carry out a transaction. Unfortunately, with the use of personal identification numbers, there is a limit to the security that can be provided. For example, in four digit personal identification number, which is the more common length of number, there are only 9,999 combinations available. Accordingly, with modern high powered computers, it is relatively easy to discover the correct personal identification number stored in any particular card.

BUREAU OMPI WIPO INTERNATIONAL

Secondly, where data is transferred from a card, it is relatively easy to tap into the line transferring the data and record the transaction. Accordingly, the transaction may be replayed an unlimited number of times, and thus in the case of funds transfer, an amount of money may be fraudulently transferred an unlimited number of times.

Additionally, it is difficult to encode data being transferred in such a way that the code cannot be relatively easily broken by unauthorised people tapping into the transfer line. Attempts have been made to overcome these problems. However, so far, none of these attempts have been totally satisfactory.

Accordingly, it is an object of the invention to provide a portable data storage and transfer device and associated terminal which ensures that the portable device is relatively secure against unauthorised use. It is also an object of the invention to provide a device which will prevent the fraudulent transfer of data by replaying a transaction an unlimited number of times. Furthermore, it is an object of the invention to provide a portable device which permits the data being transferred to be encoded, so that it is virtually impossible for an unauthorised person to decode the data. It is a further object of the invention to provide a portable device which can store and transfer data without being connected on-line to a computer, and which is particularly suitable for storing and transferring monetary amounts.

The invention achieves these objects and overcomes the problems of prior art devices by virtue of the fact that the memory means in the portable device stores a plurality of identifying characteristics and the micro-computer means selects at least one of the identifying characteristics and queries the user on the selected characteristics prior to data transfer.

The advantage of the invention is that it provides a device which is relatively secure against fraudulent use. This is because the invention permits a user of the device to be queried on one or more of a number of identifying characteristics, and this has the further advantage that the number of characteristics on which the user is queried, may be increased or decreased, depending on, for example, the type of data being transferred. If the data being transferred is of relatively limited value and/or importance, only one or a few characteristics may be selected. However, if the data is important, or of a high value,

BUREAU OMPI WIPO INTERNATIONAL

then many more characteristics may be selected. For example, in the case of a user making a small purchase, he may be queried on only one characteristic, thereby having the advantage of saving time, for example, at a checkout in a store. While on the other hand, if he is making a large purchase, many more characteristics may be selected.

Preferably, the micro-computer means randomly selects one or more of the identifying characteristics. The advantage of this feature of the invention is that it makes it more difficult for fraudulent use of the card.

In one embodiment of the invention, the number of identifying characteristics selected by the micro-computer means is dependent on the data to be transferred.

The advantage of this feature of the invention is that it permits relatively small and unimportant transactions to be carried out quicker than larger or more important transactions, thereby adding to the speed at which transactions may be carried out.

Advantageously, at least one of the identifying characteristics is variable with time.

The advantage of this feature of the invention is that it makes it more difficult for the card to be used fraudulently.

Preferably, at least some of the identifying characteristics are characteristics of the user, and at least one of the variable identifying characteristics is the users age.

The advantage of this feature of the invention is that because the characteristics relate to the user, they are relatively easily remembered.

In another embodiment of the invention, the micro-computer means comprises means to date stamp each data transfer to make it a unique transaction. The advantage of this feature of the invention is that it ensures that each transaction is a unique transaction and therefore, if repeated will be rejected because the date or time will be incorrect.

BUREAU OMPI WIPO INTERNATIONAL

In another embodiment of the invention, the computer means comprises means to update the data in the memory means at certain pre-determinad times.

The advantage of this feature of the invention is that it permits the data in the card to be updated by other pre-determined data at pre-determined times. A particular advantage of this feature of the invention is that when the device is used for the storage and transfer of monetary amounts, the balance in the card may be increased or decreased by cerain pre-determined amounts at certain pre-determined times, for example, where standing orders or the like are to be transferred.

In a further embodiment of the invention the data stored in the memory means is a monetary balance.

The advantage of this feature of the invention is that it permits the device to be used in a funds transfer system.

The present invention will be more clearly understood from the following description of some preferred embodiments thereof, given by way of example only, with reference to the accompanying drawings, in which:

Fig. 1 is a perspective view of a portable device according to the invention,

Fig. 2 is a circuit diagram of the device of Fig. 1,

Fig. 3 is a perspective view from one side of a coupling terminal, also according to the invention, for use with the portable device of Fig. 1,

Fig. 4 is a plan view of the coupling terminal of Fig. 3,

Fig. 5 is a circuit diagram of the coupling terminal of Fig. 3,

Fig. 6 is a flow diagram illustrating the operations carried out by the terminal of Fig. 3,

Fig. 7 is a circuit diagram of a coupling terminal according to another embodiment of the invention,

BUREAU OMPI WIPO INTERNATIONAL

Fig. 8 is a flow diagram for the coupling terminal of Fig. 7,

Fig. 9 is a circuit diagram of a terminal according to a further embodiment of the invention,

Fig. 10 is a flow diagram for the terminal of Fig. 9,

Fig. 11 is a circuit diagram of a coupling terminal according to a still further embodiment of the invention,

Fig. 12 is a flow diagram for the terminal of Fig. 11,

Fig. 13 is a circuit diagram of a coupling terminal according to a still further embodiment of the invention,

and

Fig. 14 is a flow diagram for the terminal of Fig. 13.

Referring to the drawings, and initially to Figs. 1 to 5, there is illustrated a portable device according to the invention for storing and transferring data according to the invention, in this case, for use in storing and transferring monetary funds. The device is indicated generally by the reference numeral 1 and is substantially card-shaped, suitable for carrying around in a person's pocket, as for example a pocket calculator. The outer dimensions of the device hereinafter referred to as the card 1 are as follows:

Length	90 mm
Width	50 mm
Thickness	13 mm

The card 1 is used in a funds transfer system and each person, organization or the like participating in the system, has a card 1. For example, each person has a consumer card into which his wages and/or other funds are transferred, and from which he may transfer funds to make purchases. Each trader, for example, has a traders card, which receives funds from the consumers card at the

BUREAU OMPI WIPO INTERNATIONAL

consumers card at the point of sale. The trader may also have a separate card from which wages are paid. All cards are substantially similar and minor differences between consumer cards, traders card and organizations card and the like are described in more detail below.

A coupling terminal 2 also according to the invention through which funds are transferred between the two cards 1 is also ptovided. Device receiving slots, in this case card-receiving slots 3 and 4 in the terminal accommodate two cards between which funds are to be transferred. Each trader and organization and the like, where funds are to be transferred has a coupling terminal. The terminals are substantially similar to each other with only minor variations. Such variations are merely to adapt the terminals to the specific type of funds transfer they are used for, and are described in more detail below.

For simplicity and ease of understanding the invention, the consumer card illustrated in Figs. 1 and 2 is initially described in detail and the remaining cards are then briefly discussed. After describing the cards, a coupling terminal, for use by a trader at the point of sale is described in detail, and then the remaining coupling terminals are briefly described.

CONSUMER CARD

Referring now to Figs. 1 and 2, the consumer card 1 comprises a housing 5 of plastics material. A memory means in this case a 4K battery powered CMOS RAM memory 7 is mounted in the housing 5. The memory 7 comprises a plurality of memory positions which are not illustrated. These positions store the following data:

a. The monetary balance in the card.
b. A serial number of the card.
c. An authenticating code which is common to and recognisable by all other cards used in the system. This code ensures that spurious cards cannot be used.
d. A plurality of static identifying characteristics of the card holder, in this case, for example, a personal identification number, specific identifying characteristics of the card holder, such as the colour of the holders eyes, the colour of his hair, height,weight and the like.

BUREAU OMPI WIPO INTERNATIONAL

e. Variable identifying characteristics of the card holder, for example his age.

f. The card holders dynamics signature, which is stored digitally.

g. The expiry date of the card.

It is envisaged that the card will store up to twenty identifying characteristics, both static and variable.

A micro-computer means in this case a single chip micro-computer 10 sold under the Trade Name Sharpe Type SM3 is mounted in the housing 5 and drives the card 1. The computer 6 comprises a central processing unit 12 which manages the operations of the card. A ROM 11 having a capacity of at least 2K bytes is linked to the central processing unit 12, and contains stored programs to direct the operation of the computer 6. A RAM 14 is also linked to the central processing unit 12. The central processing unit 12 is linked to the memory 7 and randomly selects personal identifying characteristics from the memory to query the card holder prior to a transaction to establish teh authenticity of the card and the holder. A program in the ROM 11 programmes the central processing unit 12 to query the card holder on varying numbers of personal identifying characteristics depending on the size of the transaction to be entered into. In cases of particularly large transactions, the central processing unit 12 requests the card holders dynamic signature. This is described in detail below. Means to compare a card holders response with the queried characteristics is provided by a programme stored in the ROM. The comparision is carried out in the central processing unit 12.

A clock generator 15 with a speed of 32.687 KHz controls the central processing unit 12. The clock speed is kept as low as possible to reduce the power consumption of the card 1. The central processing unit 12 is connected to an I/O driver 16.

A security means, in this case a security chip 20, is mounted in the card 1 and linked to the micro-computer 6. The micro chip 20 encodes and decodes data being transferred to and from the card 1 by a public key and secret key encription technique. Such technique is described in detail by Rivest, Shamin and Adleman in an article entitled "A method for obtaining digital signatures and public key crypto-systems" published in Communications of ACM,

BUREAU OMPI WIPO INTERNATIONAL

1,133 Avenue of the Americas, New York N.Y. 10036, February 1978 at Pages 120 to 126.

The security chip 20 comprises a 1K RAM 22 in which the public and secret keys of the card holder are stored inaccessibly. Each key is a 150 digit number. A ROM 23 having a stored programme directs the encription and decription computations, which are carried out in a central processing unit 24. The central processing unit 24 is linked to a RAM 22 and the ROM 23. An I/O driver 25 and a clock generator 26 are linked to, and control the central processing unit 24.

For security, all data stored in the memory 7 with the exception of the balance and a personal identification number of the card holder is stored in encripted form. Accordingly, on being entered into the memory 7 this data is first encripted by the security chip 20. Furthermore, when personal identifying data is entered into the computer 10 of the card 1, this is first encripted by the security chip 20 prior to being compared with the stored data in the memory 7. The two encripted forms of this data are then compared in the micro-computer 10.

A crystal 21 linked to the micro-computer 10 synchroneses the operation of the computer 10.

A digital display, in this case provided by an eight digit, seven segment liquid crystal display 10 is mounted in the housing 5 to permit the balance in the memory 7 to be displayed on request. The display 28 is linked to the micro-computer 10.

A keyboard 30 in the housing 5 and linked to the microcomputer 10 permits instructions and data to be entered into the card. The keyboard 30 comprises ten alphanumerical keys 31, namely keys 0 to 9. Two instruction keys are also provided on the keyboard 30 namely, an instruction key 32 to instruct the card to display the balance on the display 28, a command key 33 which initiates funds transfer between two cards. When the card 1 is in a terminal, the command key 33 is inoperable but the funds transfer command key 33 is used to initiate funds transfer, as described below. When the card is in a terminal, the commands are entered into the card by the keyboards on the terminal.

BUREAU OMPI WIPO INTERNATIONAL

A battery 37 in this case, a rechargable nickel cadmium battery mounted in the card 1 powers the card through the power connections 38.

Coupling means for the transfer of data between two cards through a terminal, is provided by an ultra-sonic coupling device 40. The ultra-sonic coupling device 40 is connected to the micro-computer 10 and in use, co-operates with a corresponding ultra-sonic coupling device mounted in one of the slots 3 or 4 of the terminal 2. The coupling means also includes a transformer powered coil 42 for the transfer of power from a terminal 2 to charge the battery during a transaction and also to provide additional power as required to the various components on the card during a transaction. The coupling coil 42 co-operates with a corresponding coil in one of the slots 3 or 4 in the terminal. The ultra-sonic coupling device 40 and the coupling coil 42 are both mounted internally in the card at 43, see Fig. 1. All the components in the card just described are inter-connected on a printed circuit board (not shown) and are encased in an epoxy resin to prevent tampering.

Other cards are provided for use in the system, for example, a card for a trader for use at the point of sale to receive funds from consumer cards. An official bank card is also provided for the banks to store funds for transfer to consumers cards on request. Wages payment cards are also provided. Wages payment cards store wages and the value of the wage to be transferred to each employee. These additional cards are similar to the consumer cards just described with the exception that they each have a larger memory to store many transactions, and to store a black list of invalid cards. The black list is updated on an ongoing basis where the card is in a terminal which is connected on line to a central computer containing the information, or alternatively where the card is not connected on line, the list would be updated by a bank each time a withdrawal or a lodgement was being made.

COUPLING TERMINAL

Figs. 3 to 5 illustrate the coupling terminal 2 for coupling two cards for the transfer of funds between each card. In this case, the coupling terminal 2 is a point of sales terminal and is used in a shop or store where customers puchase items and pay for them with their concumer card 1. The terminal 2 is in two

BUREAU OMPI WIPO INTERNATIONAL

portions, a consumer portion 39 and a traders portion 41 connected by cables 44. The consumer card receiving slot 3 is provided in the portion 39 and the traders card receiving slot 4 is in the portion 41. A third card receiving slot 46 in the portion 41 receives a back-up card which is a duplicate of the traders card. All transactions recorded on the traders card are duplicated on the back-up card in the event of loss or damage to the traders card.
The slot 46 houses the back-up card in a portion of the terminal, which is accessible only by a bank.

Two digital displays are provided, one on each portion 39 and 41, namely, a display 47 for the consumer and display 48 for the trader. Both displays 47 and 48 are single line displays with forty upper-case alpha numerical characters. Key boards 50 and 51 for the consumer and the trader respectively are provided. The consumers keyboard 50 comprises ten alpha numerical keys 54, a command key 55 to cancel an entry, and a data enter key 56 to enter data into the terminal. The traders keyboard 51 also comprises ten alpha numerical keys 58 (0 to 9), and a decimal point key 59. Five command keys as follows are also provided on the traders keyboard 51:

60 - a cancel entry key
61 - a data enter key
62 - a display day total key for commanding the terminal to display the total of the days transactions on the display 48
63 - a display card total key for commanding the card total to be displayed
64 - an end transaction key to terminate a transaction.

Referring now to Fig. 5 a micro-computer 65 is connected to the display 47 and 48, the keyboards 50 and 51 and the card receiving slots 2, 3 and 46 is provided in the terminal 2. The computer 65 routes data between the cards in the terminal, the keyboards 50 and 51 and the displays 47 and 48. The micro-computer 65 comprises a micro-processor 67 to control the operations of the terminal, a ROM 68 to store the control program and other permanent data, and a RAM 69 to store temporary data and to input/output interface to control the terminal peripherals.

Provision for an on-line link to a bank computer via a telephone line is provided in the micro-computer 65 and is illustrated by the broken line 70.

BUREAU OMPI WIPO INTERNATIONAL

A power supply unit 73 powered by the AC mains and a stand-by battery 74 drives the terminal 2 through a key switch 75. The key switch 75 is a three-position switch having an/off mode 76, a transaction mode 77 in which the terminal is activated for a transaction and a test mode 78 as can be seen in Fig. 5. In the test mode, the terminal carries out a self-test on all its components. This is controlled by the computer 65.

Transformer power coils (not shown) and ultra-sonic receivers and transmitters (also not shown) are provided in the consumer and traders card slots 3 and 4 respectively to facilitate transformer power coupling and ultra-sonic coupling between the cards and the slots. Both the power coils and ultra-sonic receivers and transmitters are connected to the computer 65. Such couplings will be well known to those skilled in the art and it is not intended to describe them in further detail. As already described, when a card is entered in a respective slot, power is delivered through the transformer power coupling coil to charge the battery of the card and also to provide additional power to the card during transfer of the data between cards and in particular during the encription operation. The data is then transferred through the ultra-sonic coupling receivers and transmitters.

An electronic pressure pad 79 to electronically monitor a dynamic signature is linked to the portion 39 of the terminal 2, and connected into the computer 65 to permit the dynamic signature of the card holder to be read into the computer 65 for further transfer into the consumers card for comparision with the dynamic signature stored in the memory 7 of the card and/or for signing a transaction. Such electronic pressure pads will be well known to those skilled in the art.

In use, when a card holder desires to check the balance in the memory 7 of his card, he enters his personal identification number by means of the alpha numerical keys 31 on the keyboard 30 and uses the balance key 32. The micro-computer 10 compares the entered number with that in the memory 7. If both compare the balance is displayed on the display 28. Because no encription or decription of the personal identification number or the balance is required, only a small amount of power is required which is supplied by the battery 37.

BUREAU OMPI WIPO INTERNATIONAL

Referring now to Fig. 6, when it is desired to transfer funds from the consumers card 1 to a traders card, the traders card is inserted in the slot 4 of the terminal 2. Normally, this would be inserted in the morning prior to the days transactions and left there for the day. Prior to any transaction taking place, the trader authenticates his card. The flow chart of Fig. 6 illustrates the steps carried out in authenticating the card. Firstly, on insertion the card on command from the terminal does a self-test. The micro-computer 10 in the traders card, randomly selects personal identification characteristics in the memory 7 of the card and queries the trader through the traders display 48 on the terminal 2. The trader keys in the relevant responses on the key board 51 by means of the alpha numerical keys 58 and the enter key 61. These are transmitted through the micro-computer 10 to the security chip 20 for encription and are then compared with the encripted data in the memory 7. If the traders responses compare with the stored data, the card is then enabled for the next operation, and the back-up storage card is overwritten with the contents of the traders card. If the responses do not compare, then the card is disabled.

Prior to inserting the consumers card 1 into the terminal 2, the consumer, to save time, enters his personal identification number into the card by means of the keyboard 30. If this compares with the stored personal identification number, the card is then enabled to perform the next operation in the terminal 2.

As already discussed, once the cards are inserted in the terminal 2 they are addressable only through the keyboards 50 and 51 of the terminal, with the exception of the transfer key 33 of the consumers card 1. On insertion of both cards in the terminal 2, power is transferred to the cards as required by the power coupling coils.

The consumer card on command from the terminal does a self-test. The serial number, authenticating code and expiry date of the consumers card are transferred in an encripted form from the consumers card 1 to the traders card. The computer 10 of the traders card checks that the cards serial number is not on the black list and also chechs the authenticating code and the expiry date. If there is any problem with any of these three, the card is disabled, and the transaction aborted. The computer 10 of the consumer card 1 then randomly selects personal identifying characteristics from the memory 7. The computer 10 queries the card holder on the selected characteristics through

BUREAU OMPI WIPO INTERNATIO

the display 47 on the terminal 2. The card holder enters the responses through the keyboard 50 and the responses are encripted in the security chip 20 and then compared by the computer 10 with the stored data. If they compare, the card is then enabled for the transaction.

If the personal identifying characteristics of the response do not compare, the card is disabled and the transaction aborted. In Fig. 6, the personal identifying characteristics are referred to as personal identifying data which is abbreviated to PID.

Once the comsumers card has been enabled, the trader then keys in by means of the keyboard 51 the amount of the transaction to be transferred from the consumers card to the traders card. This amount is displayed on both the traders and consumers displays 47 and 48. If both consumer and trader are in agreement, the consumer by using the transfer key 33 on his card 1, initiates the transfer. Initially, the message to be transferred which includes the amount of money and the card serial number, is date-stamped by the computer 10. This message is then encripted in the security chip 20 by using the traders public encription key. The encription computations are carried out in the central processing unit 24 of the security chip 20. The encripted message is then transferred through the micro-computer 65 of the terminal 2 to the traders card. As already explained, this transfer is made through the ultra-sonic coupling between the cards 1 and their respective slots 3 and 4. The message is then transferred into the security chip 20 of the traders card and decripted using the traders secret decription key. Again, the decription computations are carried out by the central processing unit 24 of the security chip 20 of the traders card 1. The date stamp is checked and the decripted amount is then entered in the balance of the memory 7 of the traders card and the serial number is stored. Simultaneously, the balance in the memory 7 of the consumers card 1 is reduced by a corresponding amount.

The encription process is explained in the following example below. Needless to say, this is merely an example and does not limit the invention.

BUREAU OMPI WIPO INTERNATIONAL

EXAMPLE

In this example, the amount to be transferred, the serial number and the time and date-stamp are the message represented by M. The public key and secret key of the traders card are P_t and S_t respectively. The security chip of the consumers card encripts the message to M_s giving

$$M_s = P_t(M).$$

When the encripted message M_s is received in the traders card, the security chip 20 in the traders card operates on the message with the traders secret key, thereby giving

$$S_t(M_s) = S_t(P_t(M)) = M$$

and accordingly, the decripted message is transferred to the traders balance in the memory 7 of his card.

In the case of certain transactions, where it is desired to have the consumer sign the message with his secret decription key, this may also be done using the method described in the paper of Rivest, Shamir and Adleman already referred to.

It will be appreciated that during any transaction, the number of personal identifying characteristics randomly selected by the computer for querying the card holder as already described may be varied depending on the size of the transaction. In the case of a large transaction, where the card holder should be queried on a large number of personal identifying characteristics, the amount of the transaction is keyed into the terminal 2 by the trader using his keyboard 51. The computer 10 in the consumers card 1 determines the number of characteristics on which the card holder is to be queried, makes the selection and queries the holder. The computer 10 may also request the users dynamic signature. In which case the user signs his signature on the electronic pressure pad 79. This, if desired, may also be transferred with the message M to the traders card.

It will be appreciated that the fact that each transaction is date stamped ensures that each transaction is unique, and if an attempt is made to repeat the transaction at a later time, into the traders card or any other card, it will

BUREAU OMPI WIPO INTERNATION

not be accepted by the card since the time will not compare. Needless to say, if the trader at any time during the day wishes to check his balance in the memory 7 of his card 1, this may be done by using the card total key 63. Similarly, if he wishes to check the days total at any time, the day total key 62 is used.

All data transmitted between the cards and the terminal is "echoed" by the receiver to the transmitter within 1 millisecont of the transmission taking place. If a transmission error is detected by the transmitter, it retransmits the data up to a maximum of 5 times. If after 5 attempts the error is still occurring, or if the "echo" is timed out, the transaction is aborted.

If data is transmitted between a card and the terminal where the receiver is expected to respond to the transmitter after processing the data, the response occurs within 5 milliseconds, otherwise a timeout occurs and the transaction is aborted. In the case where the communication is between cards (via a terminal), the timeout occurs after 15 milliseconds.

In carrying out a self test, the card responds within 100 milliseconds with the result of the self test. The test includes a check on the card expiry date. If the self test is unsuccessful, or if its response is timed out, then the transaction is aborted.

Referring now to Fig. 7, a coupling terminal 80 according to another embodiment of the invention is illustrated. In this case, the coupling terminal is referred to as an automatic payment terminal and is for use in an organization to transfer wages and salaries from an employers wages card to an employees comsumer card. Essentially, this terminal is substantially similar to that described with reference to Fig. 5 and similar components are identified by the same reference numerals. The main difference in the terminal 80 is the fact that the traders digital display 48 is replaced by a visual display unit 81. It also has additional links 82 and 83 which enable the micro-computer 65 to be connected to a printer and the employers computer respectively (which are not shown). Additional command keys 84 are provided to control the visual display unit 81. It is not intended to describe these keys in further detail as they will be readily apparent to those skilled in the art.

BUREAU OMPI WIPO INTERNATIONAL

Additionally, the key switch 75 as well as the on/off and self test modes 76 and 78 has two additional modes, one 85 to enable the wages to be keyed in, and a second mode 86 to enable wages to be paid, to guard against unlawful use of the terminal.

Fig. 8 illustrates a flow chart of the operations carried out between the employers wages card and the consumers card during a wages transfer. This chart is substantially similar to Fig. 6, and the operations involved should be readily apparent to those skilled in the art.

Fig. 9 illustrates a circuit diagram of another coupling terminal 90 for coupling cards 1, in this case the terminal is for use in a bank branch, and is referred to as a bank branch terminal. Again, this terminal is substantially similar to those already described and similar components are identified by the same reference numerals. In this case, the customers digital display is replaced by a visual display unit 91 and the consumers keyboard 50 as well as having numerical keys 54 also has twentysix alpha keys 92 and additional command keys 93. The command keys 93 include a cancel entry key, data entry key, bank giro key, a standing order key, a bank key, an update accounts key, a yes key, a no key and an end transaction key. The banks keyboard 51 also comprises additional command keys 94 which include a cancel entry key, a data entry key, an authorise key, a lodge cash key, an update accounts key, a back-up card key and an end transaction key. In the case of the bank branch coupling terminal 90 the banks card is inserted in the card receiving slot 4 and the bank customer enters his consumer card 1 in the card receiving slot 3.

Fig. 10 illustrates a flow chart of the operations in initializing, in other words, entering a cash balance into the consumers card. This flow chart is substantially similar to that described with reference to Fig. 6, and accordingly, the operations should be clear to those skilled in the art.

Referring now to Fig. 11 a coupling terminal 100 according to another embodiment of the inventions is illustrated. In this case, the terminal is a cash dispensing terminal for use in a bank to permit a bank customer to withdraw cash using his consumer card 1. This terminal 100 is substantially similar to those already described and again, similar components are identified by the same reference numeral. The main differences here is that a cash dispensing

BUREAU OMPI WIPO INTERNATIONAL

mechanism 101 is provided to dispense cash on request from a consumer. Such cash dispensers are well known and it is not intended to describe the dispenser in any detail. An additional command key 102 is provided to withdraw cash. A link 103 from the computer 65 enables an alarm to be raised when the terminal 100 runs out of cash. A further security alarm 104 is provided to raise an alarm should the terminal be tampered with or a spurious card be entered into the consumer card slot 3.

In this case, the banks card is inserted in the card receiving slot 4, and the consumers card is entered in the slot 3. A flow chart of Fig. 12 illustrates the operations carried out when the consumer withdraws cash from the dispenser. As this flow chart is again substantially similar to that described with reference to Fig. 6, the operation should be readily apparent to those skilled in the art.

Fig. 13 illustrates a terminal 110 according to a still further embodiment of the invention, in this case a coupling terminal for other payments. Typically, this terminal 110 could be used for making social welfare payments or state pensions or the like. This terminal is again substantially similar to those described and similar reference numerals identify similar components. The consumers keyboard 50 comprises two command keys 55, one a cancel data key and the other a data enter key. The keyboard 51 comprises the following command keys: a cancel enter key, a character insert key, a character delete key, four cursor control keys, paid roll forward key, paid roll backward key, display welfare benefit, on visual display unit key, print welfare benefit details on printer key, data enter key, end transaction key and a spare key.

A flow diagram is illustrated in Fig. 14 which illustrates the operations undertaken when a payment is being transferred from the other payments cards, for example, a state welfare card to a consumers card.

It is envisaged that as well as storing and transferring funds, the cards described could store and transfer other data, for example, data relating to national security and the like. Indeed, it is envisaged that two cards could be connected togehter via a telephone line by a suitable coupling terminal and messages could be relayed between cards in encoded form or otherwise.

BUREAU OMPI WIPO INTERNATIONAL

It will be appreciated that although the cards and terminals have been described as incorporating specific components, any other suitable components and circuitry could be used.

Furthermore, it will be appreciated that while the portable devices have been described as cards, they could be in any other suitable shape or form. Indeed, in certain cases, it is envisaged that they could be deskmounted units.

It is envisaged that coupling means for coupling the cards in the slots of the terminals other than transformer coils and ultra-sonic coupling could be used. For example, it is envisaged that inductive coupling, infrared coupling, light coupling or indeed galvanic contact couplings could be used. Indeed, it will be appreciated that means other than slots could be provided in the terminal for coupling. For example, pin and socket couplings could be used, or any other suitable means.

It will also of course be appreciated that other suitable shapes and construction of terminal could be used. Furthermore, it is envisaged in certain cases, where the cards are for storing and transferring data of limited importance, the security chip could be deleted from the card, and the message being transferred need not be encoded. It will of course be appreciated that where encoding is used, other suitable encoding and decoding techniques besides encription could be used. Furthermore, it will be appreciated that instead of using the particular type of encription and decription described, encription according to the Data Encription Standards could be used. It is also envisaged in certain cases that a battery would be sufficient for powering the operations and power coupling could be deleted. Furthermore, it is envisaged in certain cases that the cards will not be provided with keyboards, inwhich cases access would be through the keyboards of the terminal. Similarly, the display could be deleted from the cards and in certain cases, it is envisaged that only the display and a command key to enable a balance to be displayed would be provided.

Additionally, it will be appreciated that although specific micro-computers and memories have been described, other suitable computers and memories could be used. Additionally, it will be appreciated that memories of greater or lesser

BUREAU OMPI WIPO INTERNATIONAL

storage capacity could be used. Similarly, other types of batteries could be used.

Furthermore, it is envisaged that in certain cases the micro-computer in the terminal may not be required. It is envisaged that in such a case the cards themselves could manage their own transactions.

Further, it will be appreciated that although specific command and alpha numerical keys have been described for use with each coupling terminal, other command keys or alpha numerical keys could be used as desired. Furthermore, it will be appreciated that while some of the coupling terminals have been described as having visual display units, this is not necessary, digital displays could be used instead. Similarly, the digital displays could all be replaced by visual displays as desired. Indeed, in certain cases, it is envisaged that the coupling terminal could be provided without keyboards or display, in which case the keyboards and displays of the cards would be used.

While the various micro-computers have been described as having ROM's which store the program for directing the computer, other suitable means of storing the program could be used. Indeed, other programmes could also be used.

Furthermore, while the ROM of the security chip has been described as storing the public and secret keys, these keys could be stored i: any suitable location, indeed, it is envisaged that in certain cases that they could be stored in the main memory 7 of each card.

It is envisaged that in certain cases the micro-computer 10 of each card may be programmed to deduct or increase the balance on each card by certain pre-determined amounts at certain pre-determined times. For example, in the case of a consumer having a standing order which has to be paid at a particular time each month or the like, the computer would be so programmed to deduct the amount of the standing order automatically on the pre-determined day. Additionally, it will be appreciated that the person to whom the standing order is being paid would have his card programmed to incrase the balance on his card on the same day. For example, in the case of a standing order payable to a bank, the banks card would be programmed to increase the balance by the pre-

BUREAU OMPI WIPO INTERNATIONAL

determined amount on the particular day, while the bank customers consumer card would be reduced appropriately.

Furthermore, it will be appreciated that in certain cases it will not be necessary to time and date stamp the data being transferred.

It is also envisaged that as well as showing the balance the digital display on the consumers card, if desired, could show other data as well.

Furthermore, it is envisaged that in certain cases, coupling terminals could be provided with only one receiving means, for one card. It is envisaged that such terminals could be used in for example, the bank where it was desired to couple the consumers card directly to the bank computer for the transfer of funds, another use for such a coupling terminal would be in the case where it is desired to couple a card to another card, or computer, by a telephone line, in which case the coupling device would receive the card and couple it to the telephone line. The other end of the telephone line could be connected to a computer, or a similar coupling device with another card, for example a consumer card, organizations wages card or the like.

While the invention has been described with the data being transferred as including the serial number of the card, this is not necessary. It will be appreciated that it is only necessary for the serial number of the card to be transferred with the amount if it should be so desired. Furthermore, it will be appreciated that instead of the serial number of the card, the consumers bank account number could be stored in the consumer card and this could be transferred with the amount of the transaction if desired.

Furthermore, it will be appreciated that while certain identifying characteristics have been mentioned as being stored in the card, any other type of characteristics could be stored, whether they relate to the user or not.

Additionally, it will be appreciated that while it is desirable, it is not necessary for the micro-computer 10 to randomly select the characteristics for querying the holder, these could be selected in a pre-determined manner.

BUREAU OMPI WIPO INTERNATIONAL

Furthermore, it will be appreciated that while the transactions described between cards have been date and time stamped this is not necessary.

Additionally, while the coupling terminal illustrated in Figs. 2 and 3 is in two portions, it could if desired be formed as a single unit.

BUREAU OMPI WIPO INTERNATIONAL

CLAIMS

1. A portable device (1) for storing and transferring data, the device being of the type comprising memory means (7) for storing the data and an identifying characteristic to prevent unauthorised use of the device, coupling means (40) for coupling the device (1) to an external terminal (2) or other device (1) for transferring data, micro-computer means (10) to update the data in the device (1) after data transfer, means to compare an identifying characteristic entered by the user with the identifying characteristic stored in the memory means (7), and clock means (15) to drive the micro-computer (10), characterised in that the memory means (7) stores a plurality of identifying characteristics and the micro-computer (10) selects at least one of the identifying characteristics and queries the user on the selected characteristic prior to data transfer.

2. A device as claimed in claim 1 characterised in that the micro-computer means (10) randomly selects one or more of the identifying characteristics.

3. A device as claimed in claim 1 or 2 characterised in that the number of identifying characteristics selected by the micro-computer means (10) is dependent on the data to be transferred.

4. A device as claimed in any preceding claim characterised in that at least one of the identifying characteristics is variable with time.

5. A device as claimed in any preceding claim characterised in that at least some of the identifying characteristics are characteristics of the user, and at least one of the variable identifying characteristics is the users age.

6. A device as claimed in any preceding claim characterised in that the micro-computer means (10) comprises means to date stamp each data transfer to make it a unique transaction.

7. A device as claimed in claim 6 characterised in that the micro-computer means (10) comprises means to time stamp each data transfer.

BUREAU OMPI WIPO INTERNATIONAL

8. A device as claimed in any preceding claim characterised in that the computer means (10) comprises means to update the data in the memory means (7) at certain pre-determined times.

9. A device as claimed in any preceding claim characterised in that the data stored in the memory means (7) is a monetary balance.

BUREAU OMPI WIPO INTERNATIONAL

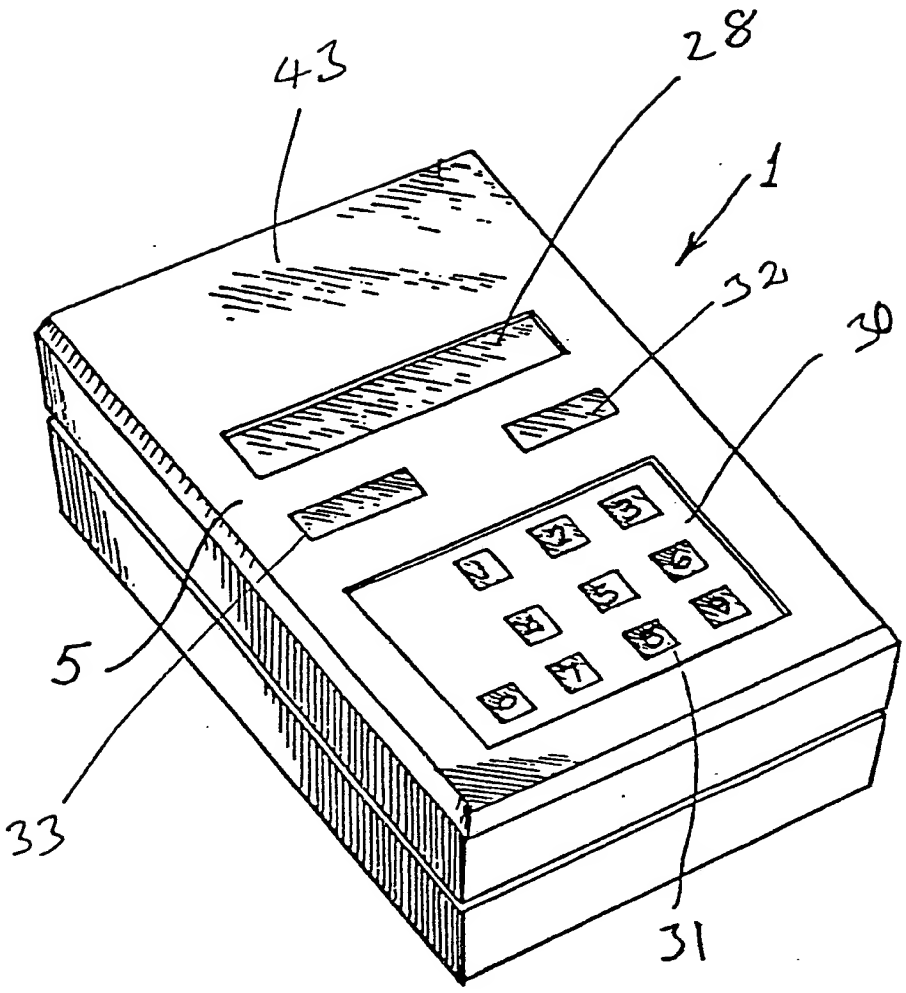


Fig. 1

BUREAU OMPI WIPO INTERNATIONAL

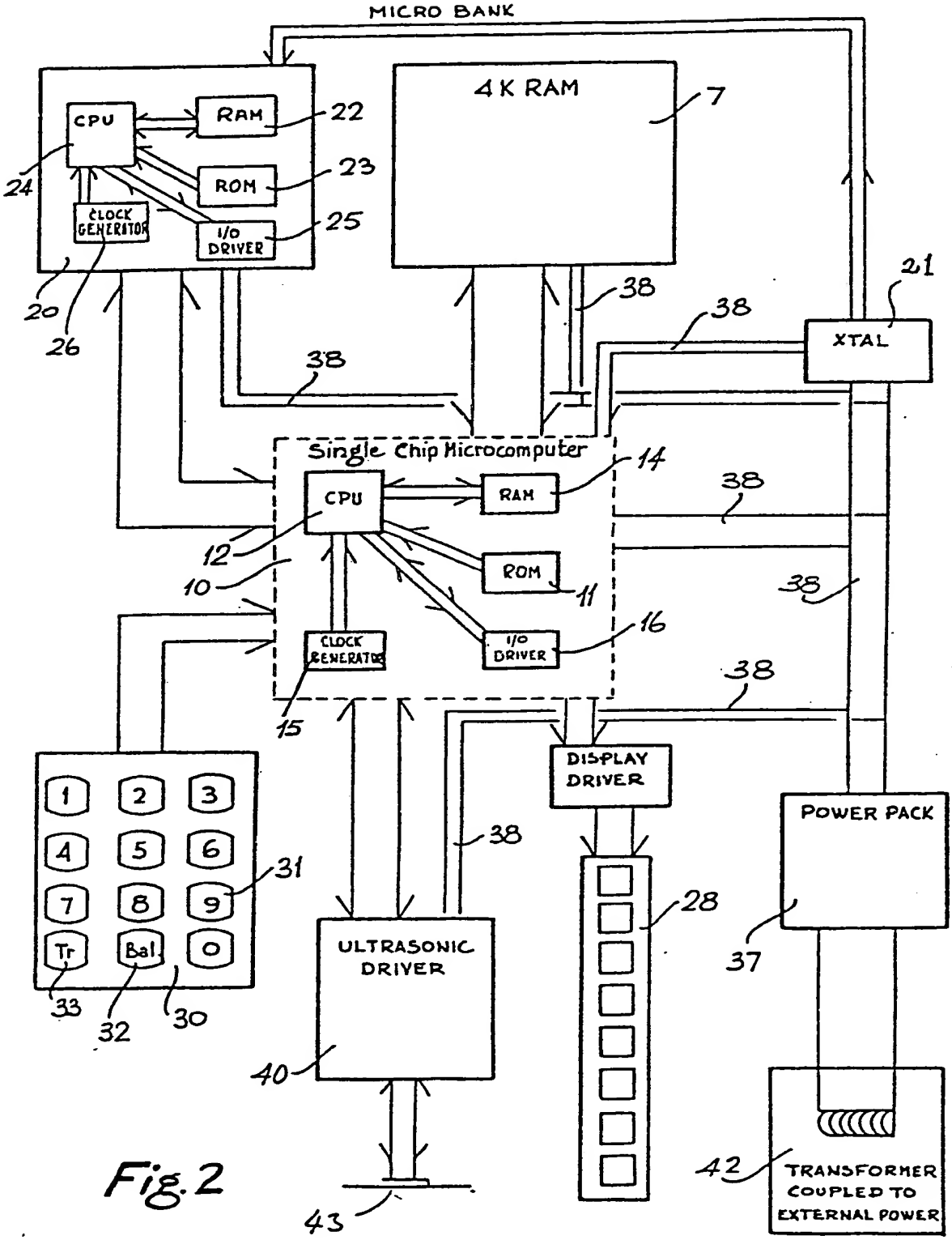
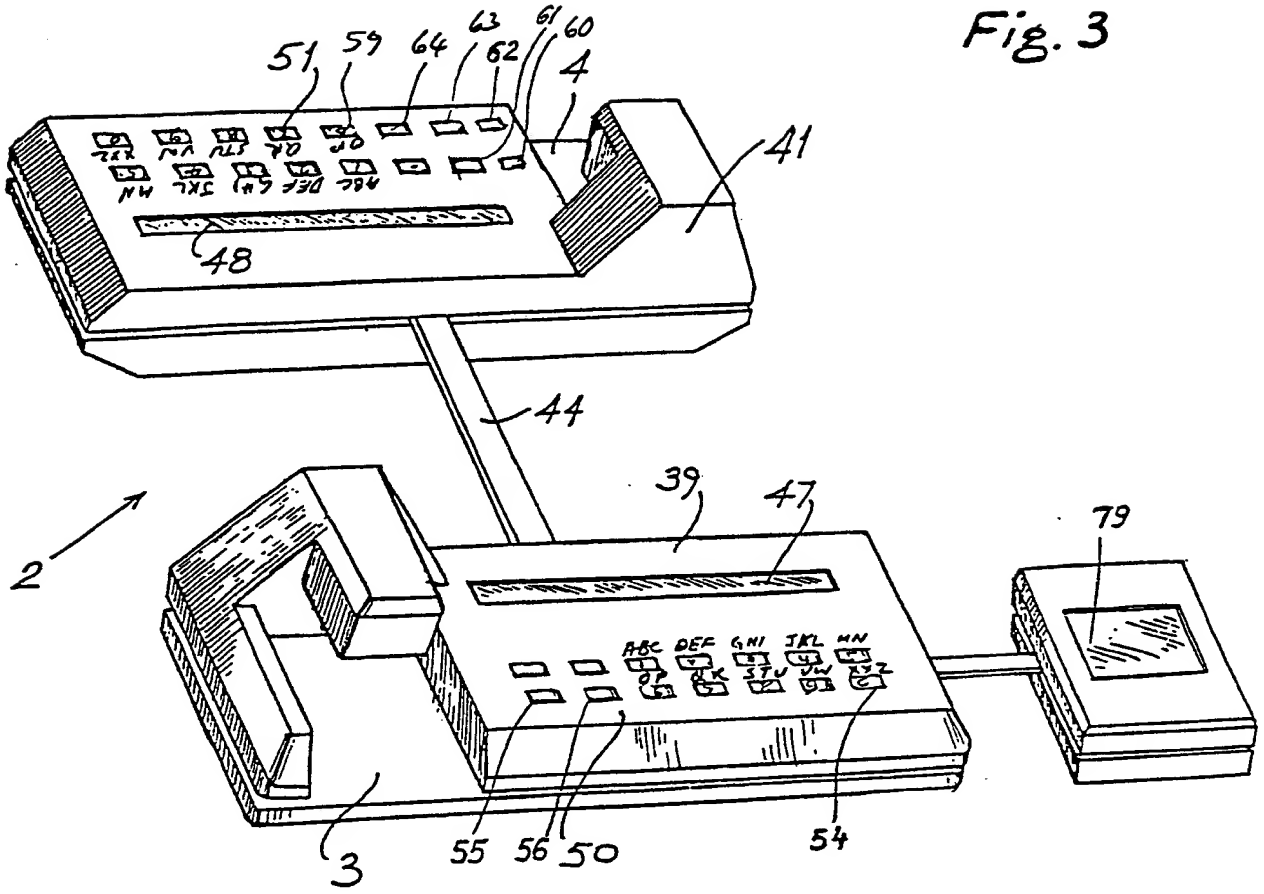


Fig. 2

BUREAU OMPI WIPO INTERNATIONAL

Fig. 3



BUREAU OMPI WIPO INTERNATIONAL

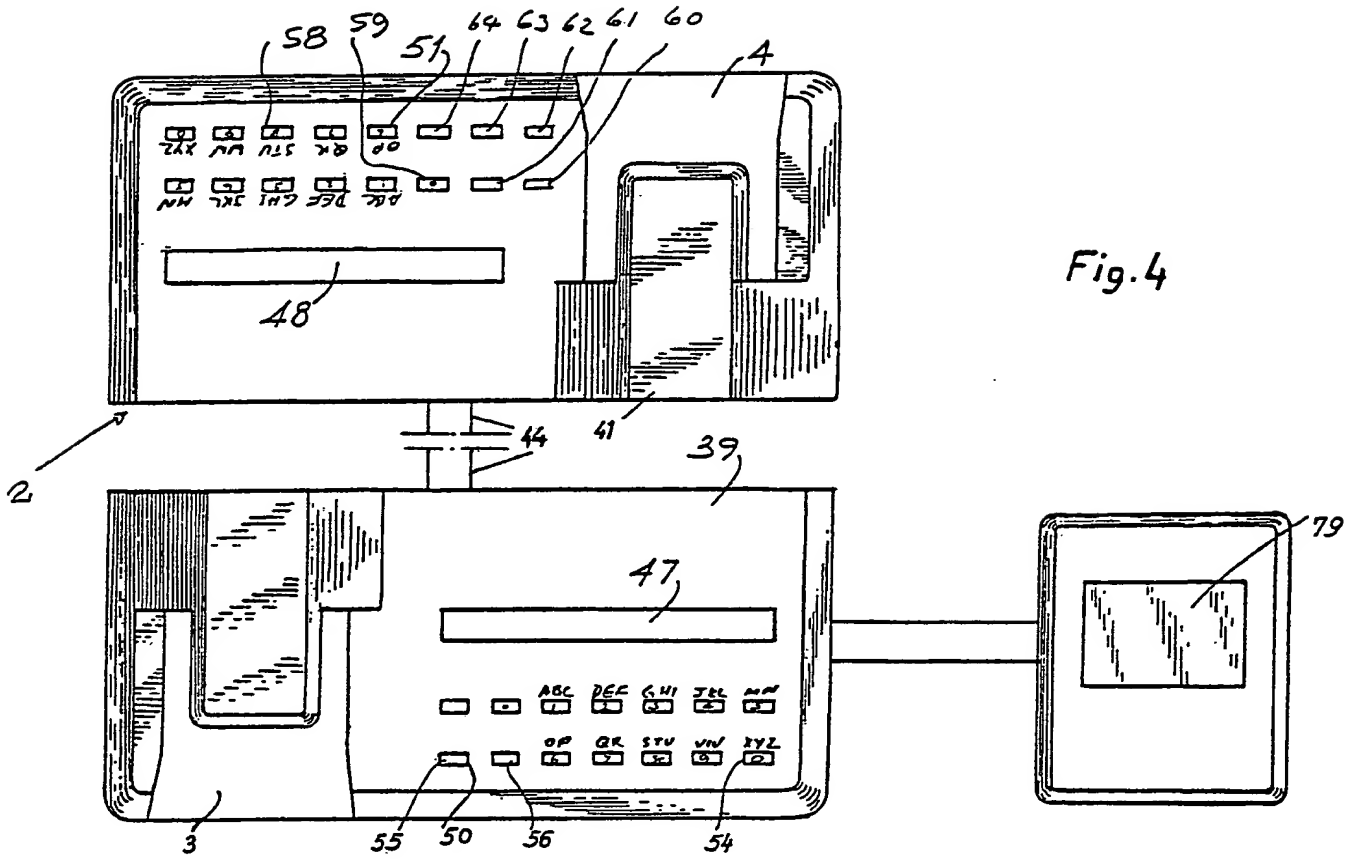


Fig.4

BUREAU OMPI WIPO INTERNATIONAL

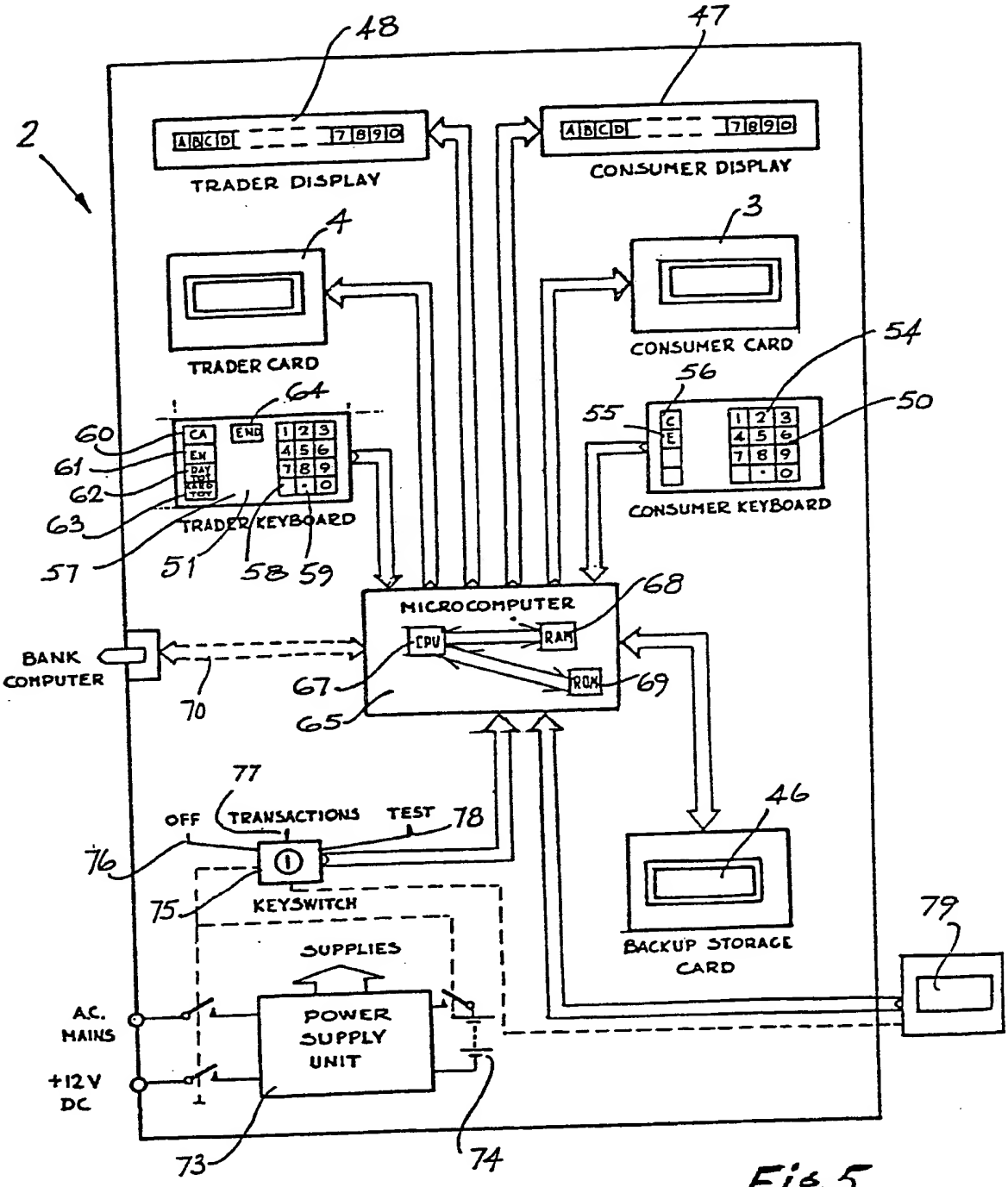


Fig.5

BUREAU OMPI WIPO INTERNATIONAL

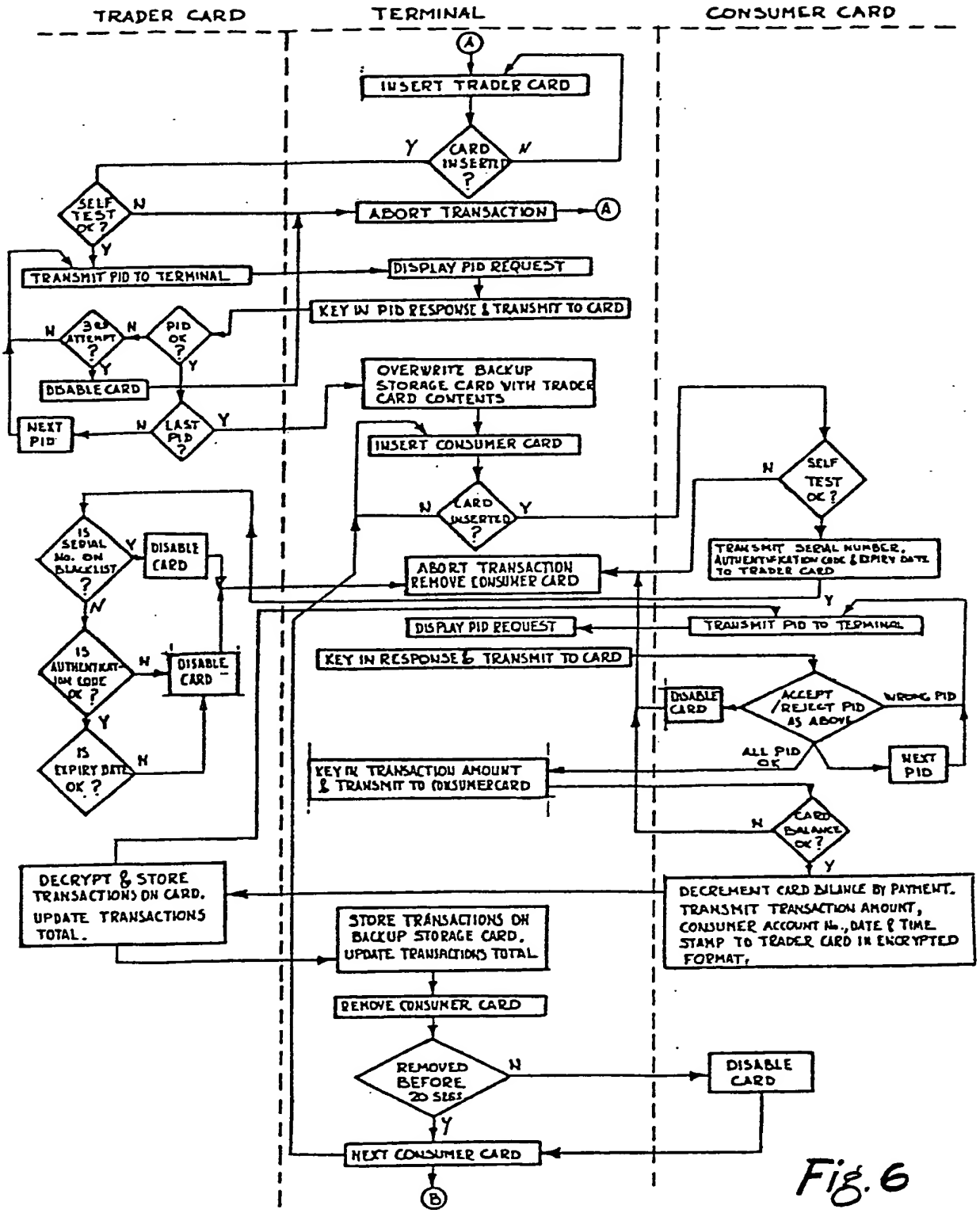


Fig. 6

BUREAU OMPI WIPO INTERNATIONA

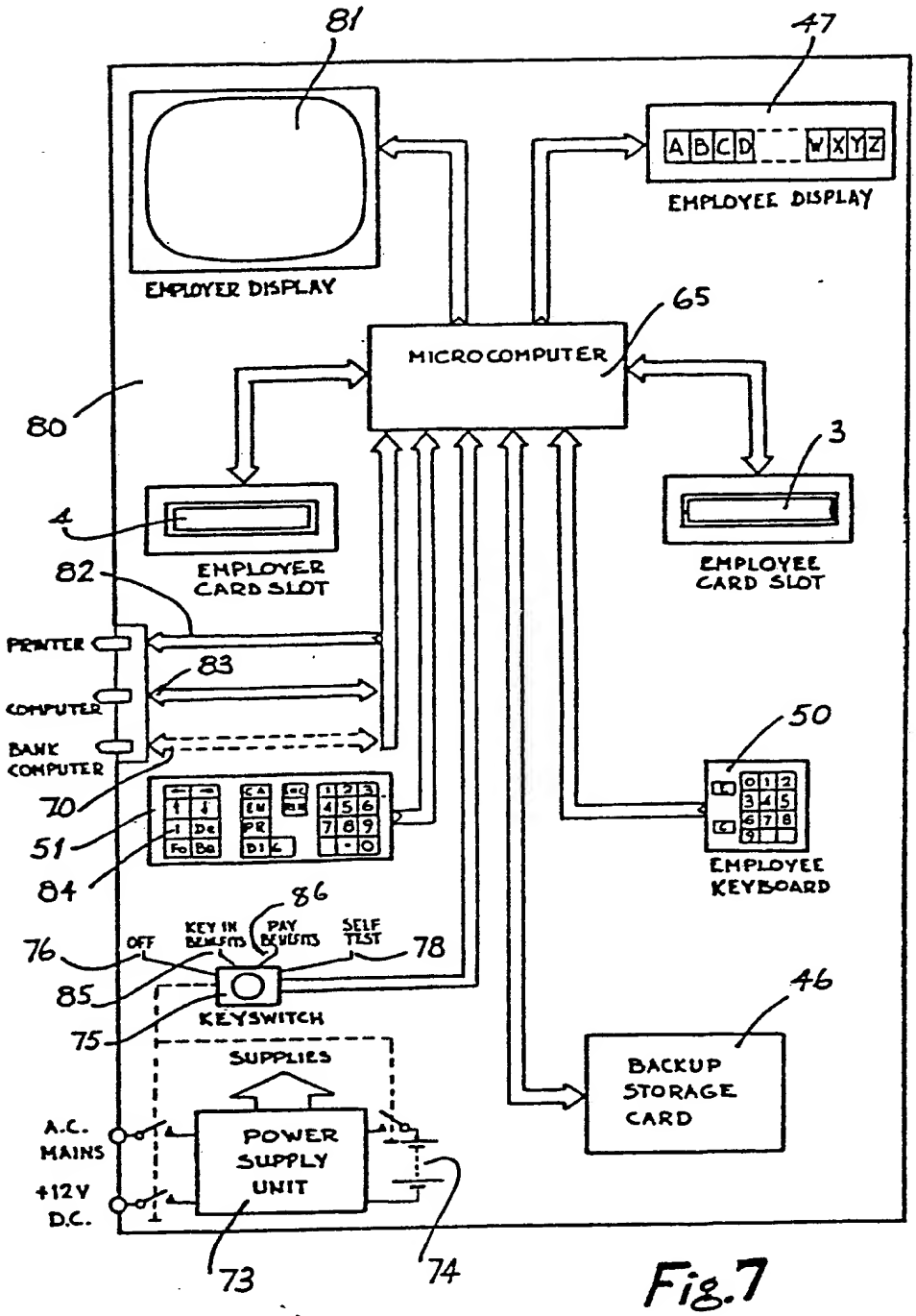


Fig.7

BUREAU OMPI WIPO INTERNATIONAL

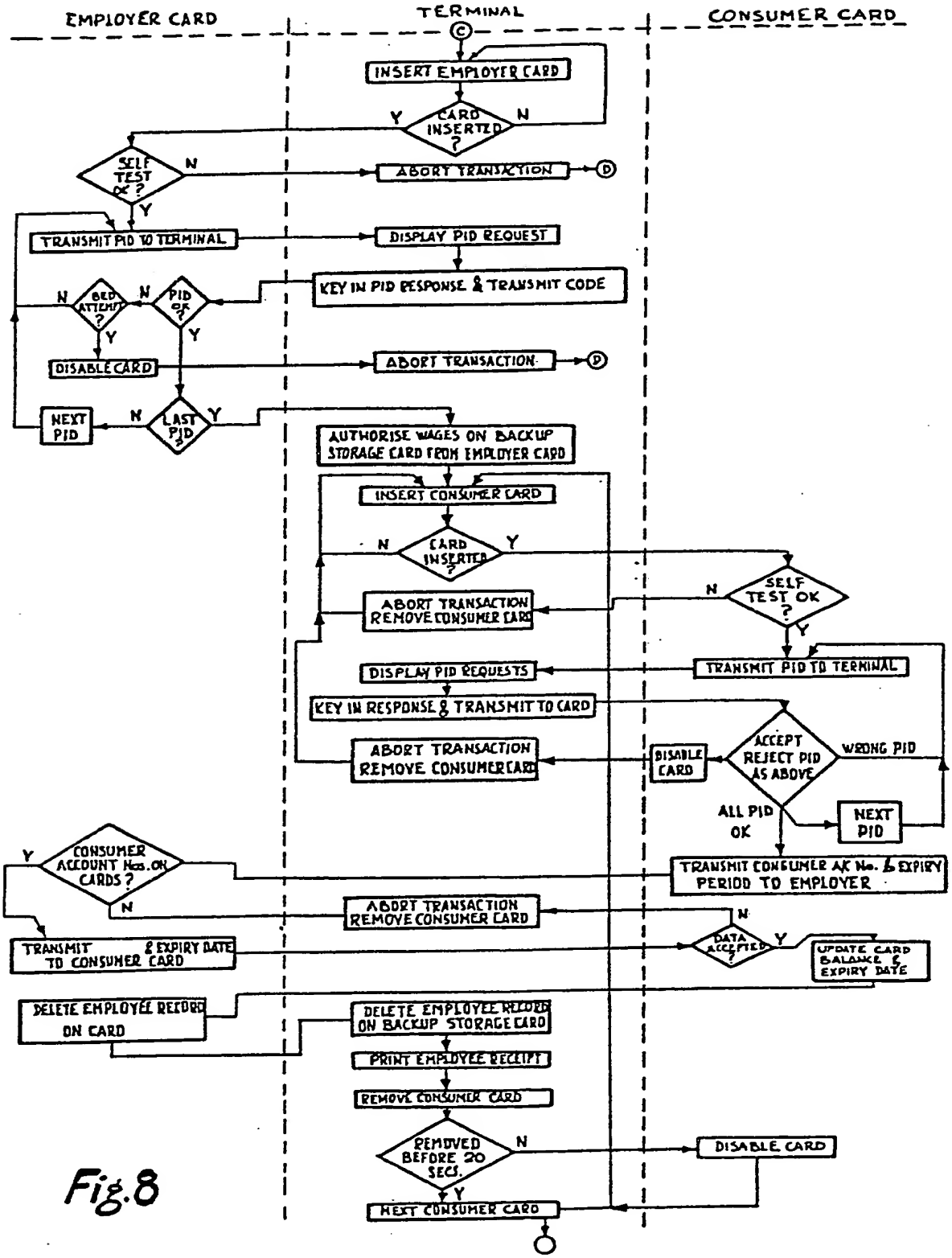


Fig.8

BUREAU OMPI WIPO INTERNATIONAL

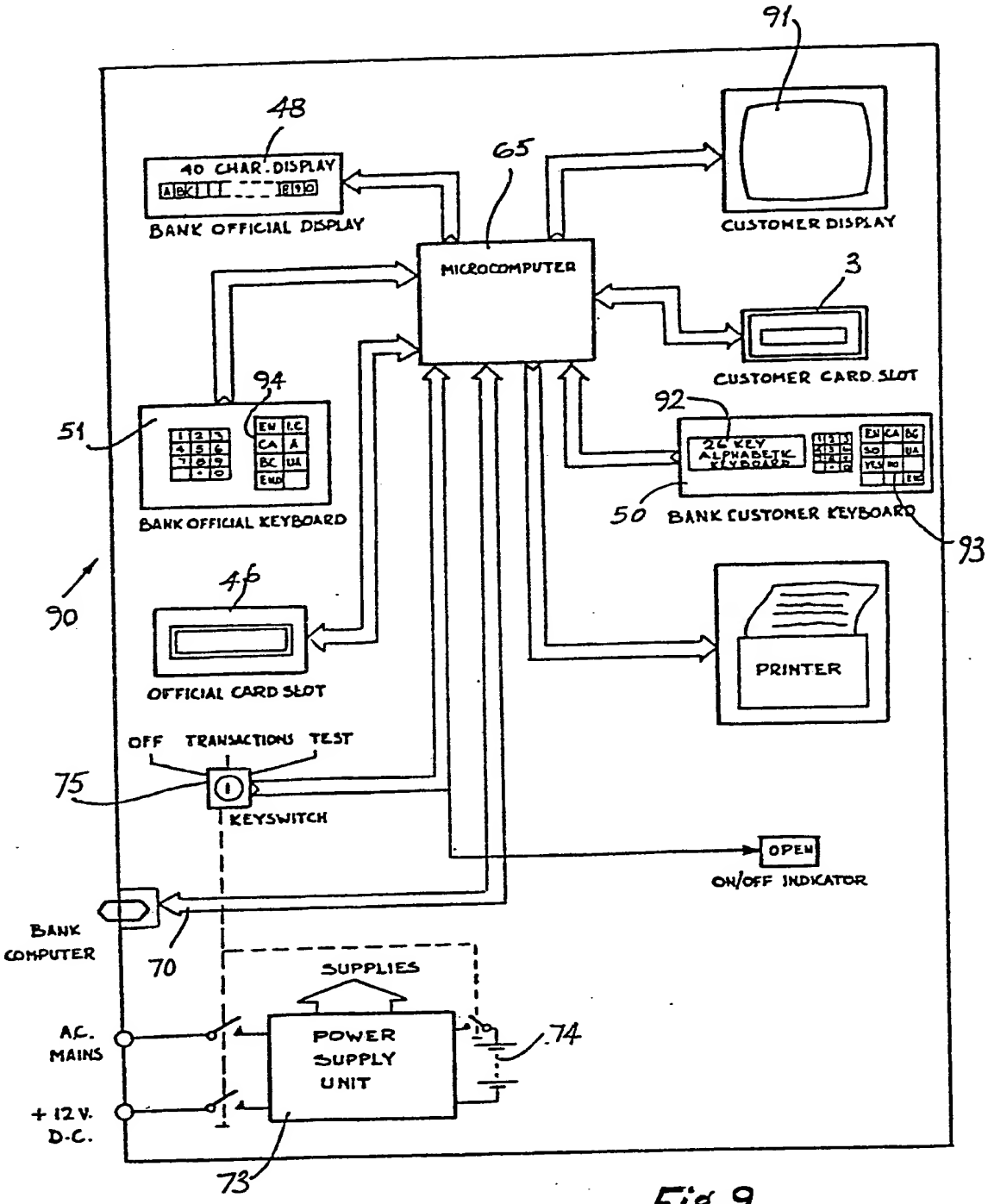


Fig. 9

BUREAU OMPI WIPO INTERNATIONAL

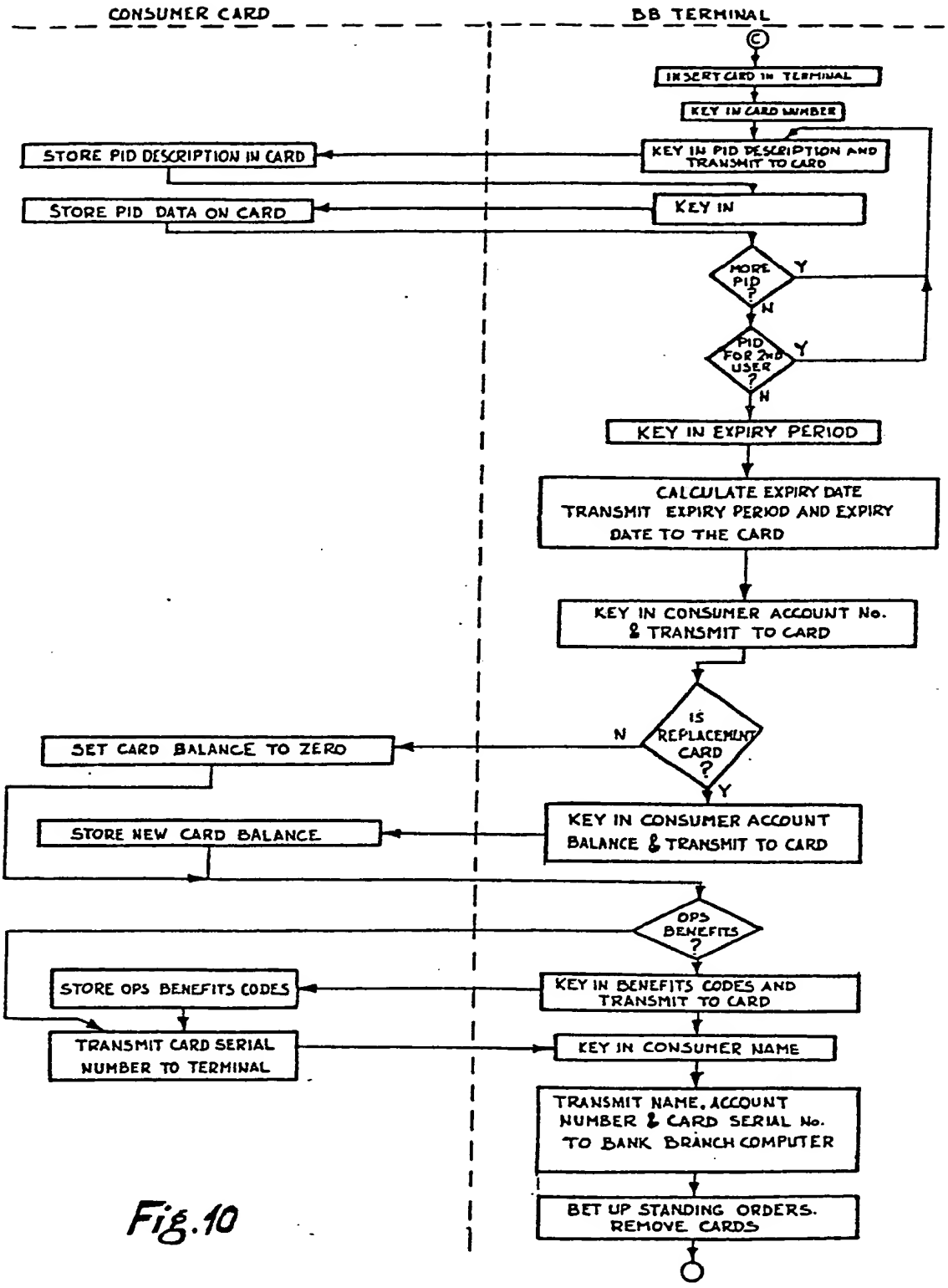


Fig. 10

BUREAU OMPI WIPO INTERNATIONAL

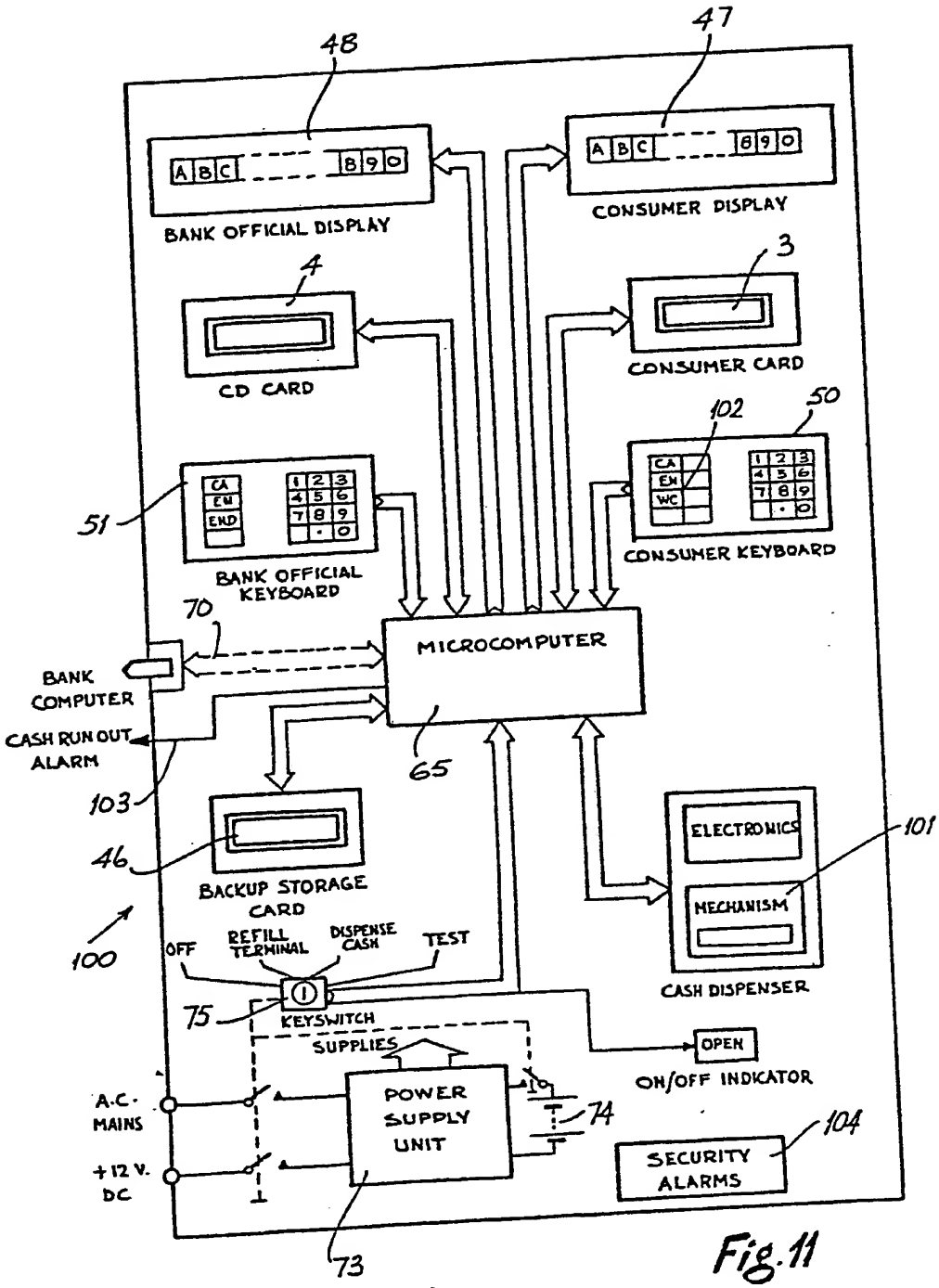


Fig. 11

BUREAU OMPI WIPO INTERNATIONAL

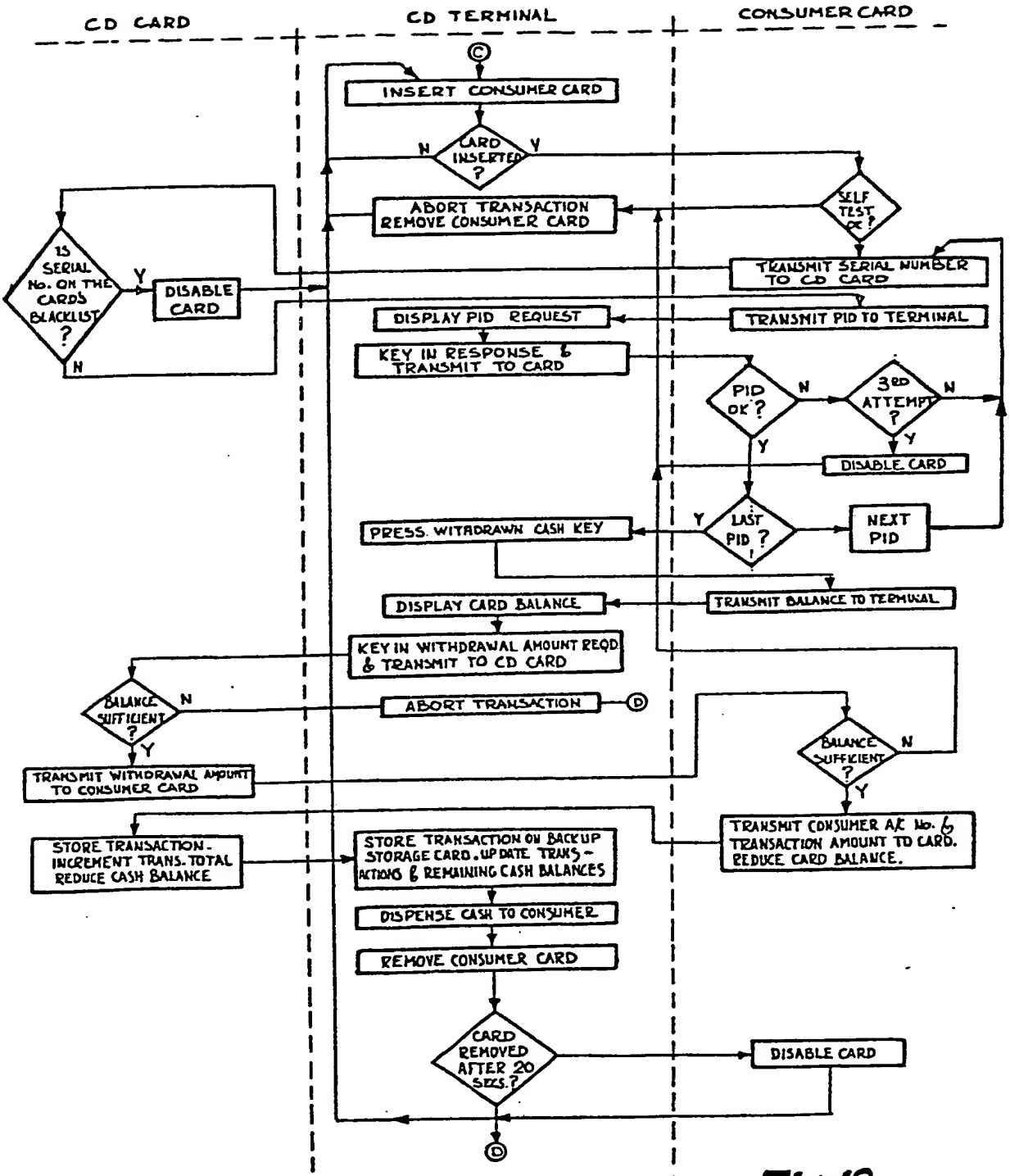


Fig. 12

BUREAU OMPI WIPO INTERNATIONAL

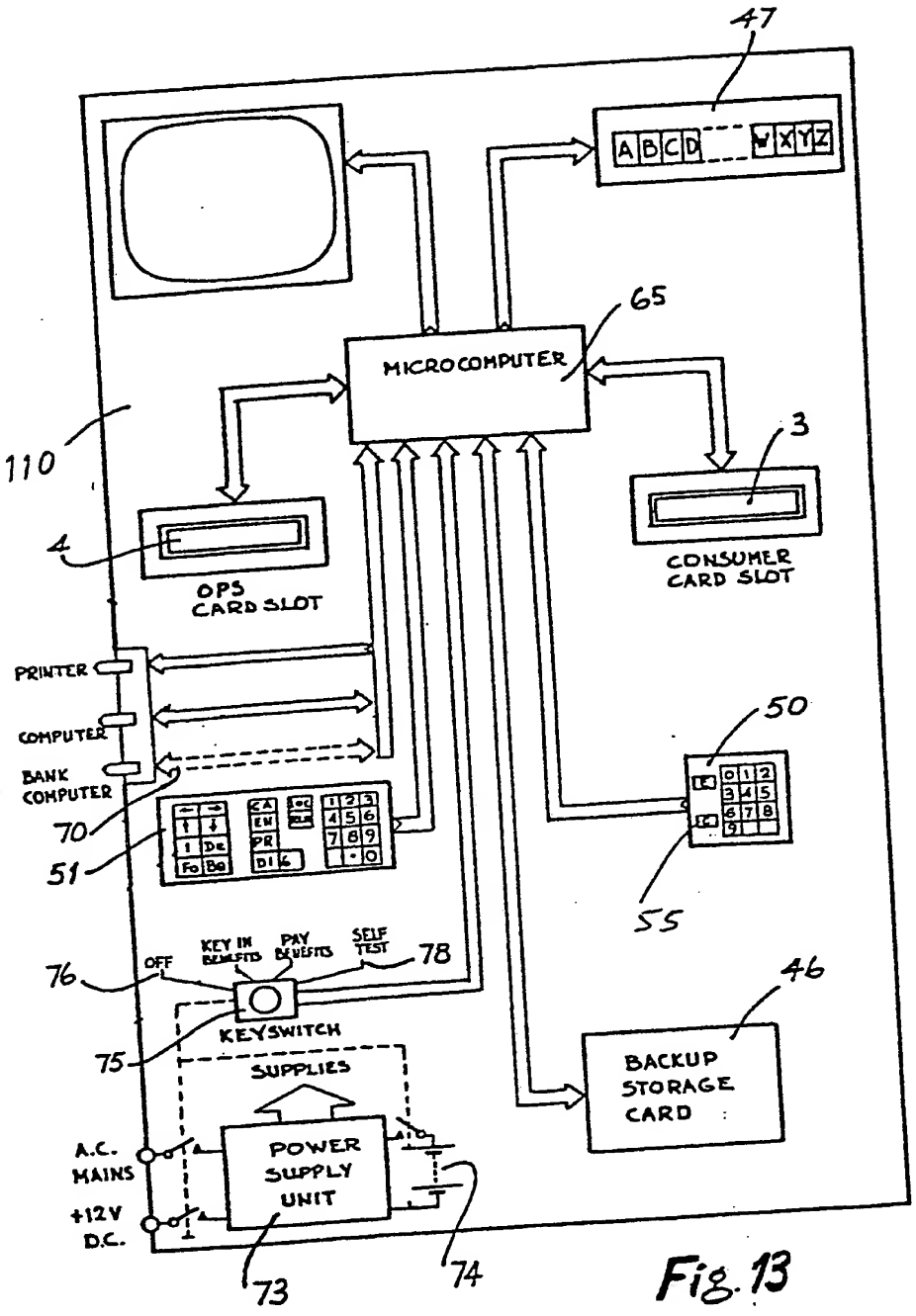


Fig. 13

BUREAU OMPI WIPO INTERNATIONAL

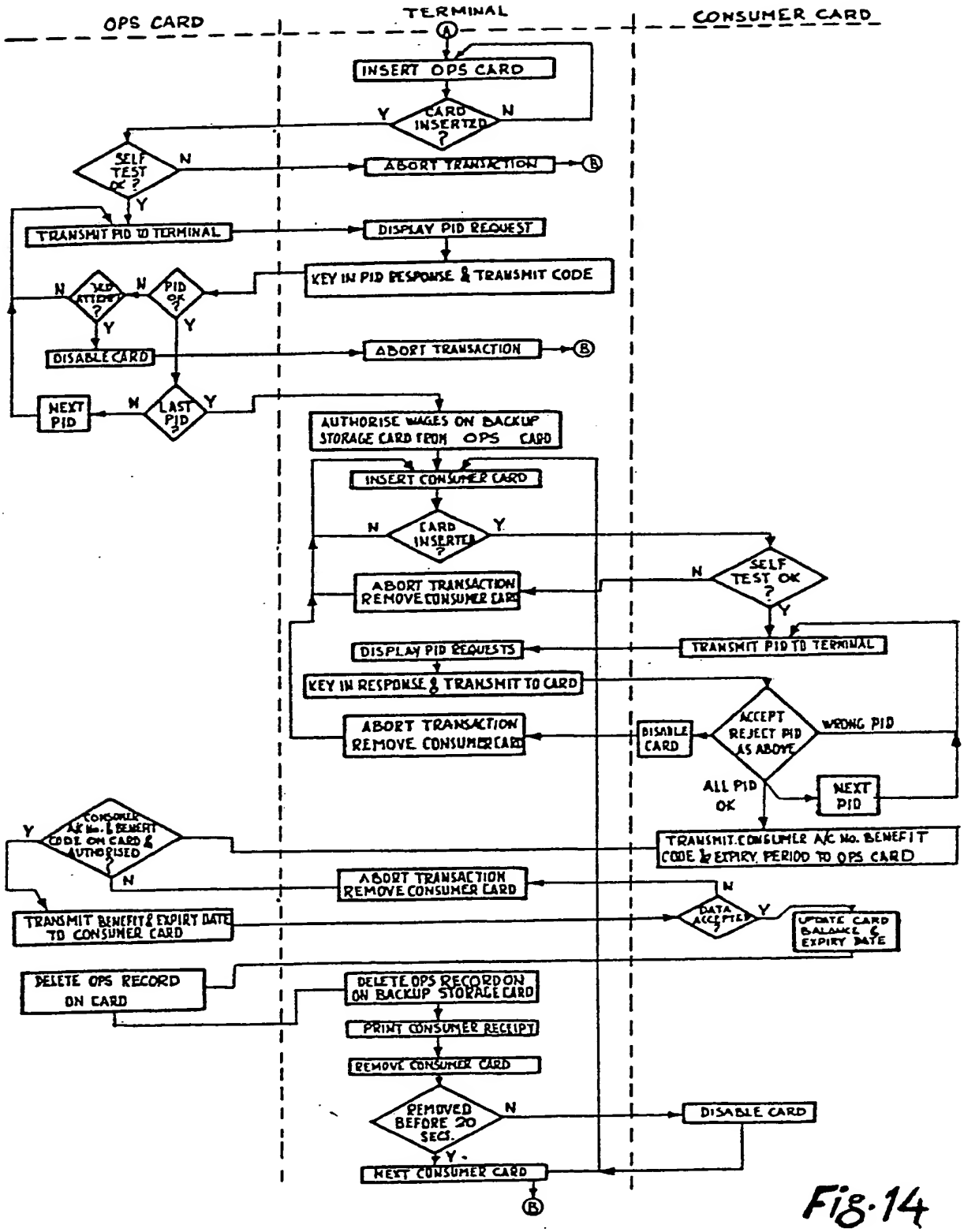


Fig. 14

BUREAU OMPI WIPO INTERNATIONAL

INTERNATIONAL SEARCH REPORT

International Application No PCT /SE83/00062

I. CLASSIFICATION OF SUBJECT MATTER (if several classification symbols apply, indicate all) [3]

According to International Patent Classification (IPC) or to both National Classification and IPC 3

G 07 F 7/10

II. FIELDS SEARCHED

Minimum Documentation Searched [4]

Classification System	Classification Symbols
IPC 3	G 07 F 7/00, /02, /08, /10, G 07 C 11/00, G 06 F 15/30, H 04 L 9/00, /02
US Cl	235:61.7B, 379, 380, 382; 340:149, 152, 153

Documentation Searched other than Minimum Documentation to the Extent that such Documents are included in the Fields Searched [5]

SE, NO, DK, FI classes as above

III. DOCUMENTS CONSIDERED TO BE RELEVANT [14]

Category *	Citation of Document, [16] with indication, where appropriate, of the relevant passages [17]	Relevant to Claim No. [18]
Y	WO, A1, 82/00213 (BENTON W M) 21 January 1982	1, 8, 9
P	WO, A1, 82/02446 (TRANSAC-ALCATEL) 22 July 1982	1, 8, 9
Y	EP, A1, 0 032 193 (IBM CORP) 22 Jly 1981	1, 6-9
Y	SE, A , 426 190 (EKONOM PANEL AB) 3 September 1980	1, 6-9
Y	GB, A , 2 066 540 (W LETMABY & CO LTD) 8 July 1981	1, 6-9
P	GB, A , 2 092 343 (DAVID A CHALMERS) 11 August 1982	1, 8, 9
Y	US, A , 3 971 916 (SOC INTERNATIONAL) 27 July 1976	1, 8, 9
Y	US, A , 4 007 355 (SOC INTERNATIONAL) 8 February 1977	1, 8, 9

.../...

* Special categories of cited documents: [15]

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

IV. CERTIFICATION

Date of the Actual Completion of the International Search [2]	Date of Mailing of this International Search Report [2]
1983-05-06	1983 -06- 01
International Searching Authority [1]	Signature of Authorized Officer [20]
Swedish Patent Office	C A Lannefors

See notes on accompanying sheet

III. DOCUMENTS CONSIDERED TO BE RELEVANT (CONTINUED FROM THE SECOND SHEET)

Category *	Citation of Document, [16] with indication, where appropriate, of the relevant passages [17]	Relevant to Claim No [18]
Y	US, A , 4 092 524 (SOC INTERNATIONAL) 30 May 1978	1, 8, 9
Y	US, A , 4 211 919 (CIC) 8 July 1980	1, 8, 9
Y	US, A , 3 876 864 (DIEBOLD INC) 8 April 1975	

This Page Blank (uspto)